Dificuldades na implementação de segurança da informação no serviço público brasileiro: a responsabilidade da alta administração

Adriana Marcilio[1], Rafael Rabelo Nunes[2]

drimarcilio@hotmail.com; rafaelrabelo@unb.br

[1] Universidade de Brasilia (UnB), Campus Darcy Ribeiro, Departamento de Engenharia Elétrica, CEP: 70910-900 Brasilia - DF Brasil

[2] Universidade de Brasilia (UnB), Campus Darcy Ribeiro, Departamento de Engenharia Elétrica, CEP: 70910-900 Brasilia - DF Brasil

DOI:

Resumo: Este artigo analisa os desafios para a implementação da segurança da informação no serviço público brasileiro, com ênfase na responsabilização da alta administração. Para isso, a pesquisa utiliza a Teoria do Enfoque Meta-analítico Consolidado (TEMAC) como método de revisão sistemática da literatura. Os resultados apontam omissões normativas, fragilidade das estruturas de governança e baixa participação da alta gestão nos processos decisórios de segurança da informação. Evidências nacionais e internacionais indicam a ausência de atribuições formais de responsabilidade e obstáculos legais à responsabilização administrativa. Constata-se que a ausência de governança e accountability influenciam diretamente na limitação da implementação das políticas públicas de segurança da informação. O estudo contribui para o mapeamento de entraves regulatórios e institucionais, e sugere caminhos para o aprimoramento das políticas públicas e de responsabilização no alto escalão.

Palavras-chave: Cibersegurança; Segurança Cibernética; Órgãos Públicos; Dificuldades; Accountability;

Challenges in implementing information security in the Brazilian public sector: the accountability of senior management

Abstract: This article examines the challenges to implementing information security in the Brazilian public sector, with an emphasis on the accountability of top management. For this purpose, the study adopts the Consolidated Meta-

Analytical Approach Theory (TEMAC) as a method for conducting a systematic literature review. The results reveal regulatory omissions, weak governance structures, and limited participation of senior leadership in decision-making related to information security. National and international evidence indicates the absence of formal responsibility assignments and legal barriers to administrative accountability. The lack of governance and accountability is found to directly obstruct the implementation of public information security policies. This study contributes to mapping regulatory and institutional barriers and suggests pathways for improving public policies and executive-level accountability.

Keywords: Cybersecurity; Public Agencies; Challenges; Accountability.

1. Introdução

A transformação digital e a crescente dependência de sistemas informacionais no setor público brasileiro elevaram a segurança da informação à condição de tema estratégico para a administração pública. O aumento dos incidentes cibernéticos, evidenciado pelo crescimento de ataques no Brasil e no mundo devido à expansão da conectividade e digitalização (Nakamura, 2024), aliado à complexidade dos ambientes digitais e à necessidade de proteger dados pessoais e institucionais, impõe desafios significativos à gestão pública. Nesse cenário, a implementação efetiva de políticas e controles de segurança da informação (Ferreira, 2022) é essencial para assegurar a continuidade dos serviços públicos, manter a confiança da sociedade e preservar a soberania digital do país, especialmente diante da ausência de coordenação centralizada (Serpa, 2024) e de estratégias integradas para prevenção e resposta a incidentes cibernéticos.

A literatura nacional e internacional demonstra que a responsabilização da alta administração pela segurança da informação ainda é insuficientemente abordada tanto nos normativos quanto na prática institucional. Trabalhos como os de (Vatamanu & Tofan, 2025) apontam que a eficácia de políticas públicas de cibersegurança depende da existência de controles e sanções aplicáveis em todos os níveis hierárquicos, incluindo os cargos de direção. A ausência de responsabilização

da alta administração compromete diretamente a resiliência organizacional frente a incidentes (Magnusson, Dalipi, & Elm, 2023).

No contexto brasileiro, a situação é agravada pela baixa maturidade institucional e pela limitada presença de lideranças técnicas em segurança da informação. Estudos nacionais (Georg, Rodrigues, Alves, Silveira Júnior, & Nunes, 2022) (Santiago Paz, 2025) revelam o distanciamento dos dirigentes máximos das decisões estratégicas de TI e a carência de estruturas formais de governança cibernética. A análise dos Acórdãos do TCU 2.387/2024 (Tribunal de Contas da União, 2024) e 2.430/2024 , (Tribunal de Contas da União, 2024) evidencia a necessidade de aperfeiçoamento normativo, de modo a explicitar a responsabilidade da alta administração na gestão dos riscos cibernéticos.

Identifica-se, portanto, uma lacuna importante na literatura. Embora existam estudos mapeando desafios gerais e reconhecendo a relevância do engajamento gerencial, ainda é limitada a pesquisa científica que aprofunde a questão específica da responsabilidade da alta administração na segurança da informação do setor público brasileiro. Grande parte das publicações concentra-se em aspectos técnicos ou em diagnósticos amplos, sem abordar de forma sistemática como os dirigentes públicos influenciam a implementação das políticas de segurança.

Diante desse contexto, o presente trabalho tem como objetivo analisar em profundidade as dificuldades enfrentadas na implementação da segurança da informação no serviço público brasileiro, com ênfase na responsabilidade e no papel exercido pela alta administração nesse processo.

A metodologia TEMAC foi empregada para consolidar achados de pesquisas anteriores e analisar a atuação da alta gestão nesse contexto.

Além de consolidar achados teóricos a pesquisa pretende auxiliar gestores públicos na identificação de fragilidades normativas e institucionais que dificultam a

implementação de medidas eficazes. As evidências visam contribuir para políticas públicas mais alinhadas à responsabilização executiva.

2. Fundamentação teórica

Nessa seção apresentam-se os conceitos necessários para que se compreenda este trabalho.

A alta administração é composta pela autoridade máxima de uma organização pública e pelos dirigentes superiores, responsáveis por avaliar, direcionar e monitorar a atuação institucional (Tribunal de Contas da União, 2020). No âmbito do Poder Executivo federal, conforme estabelecido pelo Decreto nº 9.203/2017 (Brasil, 2017), integram a alta administração os Ministros de Estado, ocupantes de cargos de natureza especial, de nível 6 do Grupo-Direção e Assessoramento Superiores (DAS), além de presidentes e diretores de autarquias, inclusive as especiais, fundações públicas ou autoridades de hierarquia equivalente. Essas funções estão diretamente relacionadas à formulação de políticas, à definição de objetivos e ao direcionamento estratégico das organizações públicas.

No campo da tecnologia e da gestão de dados, a segurança da informação é definida como o conjunto de políticas, normas e procedimentos voltados à proteção da informação contra acessos não autorizados, alterações indevidas ou indisponibilidade. Fundamenta-se nos princípios da confidencialidade, integridade e disponibilidade (ABNT, 2023). A cibersegurança, embora relacionada à segurança da informação, tem escopo mais específico: consiste na proteção de ativos digitais e infraestrutura tecnológica contra ataques e incidentes no ciberespaço (ABNT, 2023).

Complementarmente, a privacidade refere-se ao direito dos titulares de dados de controlar o uso e compartilhamento de suas informações pessoais, como estabelecido na Lei Geral de Proteção de Dados (Brasil - Presidência da República, 2018).

A Governança pública, por sua vez, é o sistema pelo qual as instituições são dirigidas, monitoradas e avaliadas, englobando liderança, estratégias e mecanismos de controle que de modo a aumentar as chances de entrega de bons resultados aos cidadãos, em termos de serviços e políticas públicas (Tribunal de Contas da União, 2020). O *compliance* é entendido como a conformidade das ações organizacionais com normas legais, regulamentos internos e códigos de conduta, buscando evitar desvios, fraudes e riscos reputacionais (Silva & Santos, 2020). Já o *accountability* representa obrigação de responder por atos administrativos (*answerability*) bem como inclui mecanismos de responsabilização (*enforcement*) que asseguram a aplicação de sanções sempre que os padrões de integridade não forem cumpridos (OECD – Organisation for Economic Co-operation and Development, 2020)

A responsabilização administrativa no setor público federal é regida pela Lei nº 8.443/1992 (Presidência da República, 1992), exigindo a comprovação de nexo causal entre a conduta do agente e o dano causado ao erário, bem como a demonstração de dolo ou culpa para aplicação de sanções. Esse modelo embasa a atuação do TCU também no campo da segurança da informação. (Tribunal de Contas da União, 2024).

A maturidade em segurança da informação foca na avaliação e gestão do grau de proteção dos sistemas no ambiente de privacidade e cibernético (Brasil - Secretaria de Governo Digital, 2023). No setor público federal, essa maturidade é avaliada por meio do Programa de Privacidade e Segurança da Informação – PPSI -, conduzido pela Secretaria de Governo Digital (Brasil. Ministério da Gestão e da Inovação em Serviços Públicos, 2023). O modelo PPSI foi estruturado tomando como base o CIS *Critical Security Controls* e orienta que os órgãos públicos adotem as medidas do nível IG1 do CIS, voltadas à proteção básica contra ataques cibernéticos. Uma vez alcançado o nível IG1, as organizações devem avaliar a criticidade de seus sistemas e determinar a necessidade de adoção dos próximos níveis IG2 e IG3 (Brasil - Secretaria de Governo Digital, 2023).

A literatura científica sobre segurança da informação no setor público brasileiro evidencia que os desafios de implementação de medidas de segurança da informação são multifatoriais e interdependentes. A ausência ou insuficiência de políticas institucionais de segurança, a falta de uma política de segurança da informação institucionalizada (Santos & Silva, 2021) e a baixa maturidade das estruturas de governança manifesta-se tanto na dificuldade de integração entre gestão de risco cibernético e corporativo, resultando em governança fragmentada em silos (Alves, Georg, & Nunes), quanto na baixa maturidade na gestão de riscos digitais observada nas administrações públicas brasileiras (Ribeiro & Segatto, 2025).

Outra dificuldade reside na desconexão entre normas e práticas. Normativos de cibersegurança ou privacidade brasileiros, no geral, são redigidos em grau de abstração tão elevado que pouco dialoga com as rotinas dos órgãos públicos, gerando, muitas vezes, mera conformidade formal (Nakamura, 2024). Como exemplo é Lei Geral de Proteção de Dados – LGPD - (Brasil - Presidência da República, 2018), cuja implementação avança de forma lenta e fragmentada, permanecendo em níveis iniciais de maturidade (Serpa, 2024).

Adicionalmente, limitações de pessoal e orçamento impactam a capacidade de implementação. A alta rotatividade de equipes, agravada pela dificuldade de manter talentos em serviços públicos diante de ofertas salariais mais atrativas no setor privado, compromete a continuidade dos projetos de segurança (Laginestra, 2021). A limitação de orçamento, com a falta de investimentos contínuos em manutenção e atualização de sistemas de segurança, impede o fortalecimento de controles e aumenta a exposição a vulnerabilidades (Laginestra, 2021).

Apesar de a modernização dos sistemas ser essencial, muitos órgãos públicos ainda operam com equipamentos defasados e softwares desatualizados, além de não adotarem processos padronizados de TI, o que aumenta a superfície de ataque e dificulta a implementação de controles mínimos de segurança (Alves, Georg, & Nunes).

A governança fragmentada ou imatura são fatores que estão presentes. A literatura evidencia que "o Brasil desenvolveu uma miríade de legislações relativas ao seu ciberespaço, embora desconexas e com implementações nebulosas" (Goldoni, Rodrigues, & Medeiros, 2023).

3. Metodologia

O presente estudo é de natureza exploratória, pois visa identificar os o problema e construir hipóteses a partir da análise da literatura científica (Gil, 2017). A abordagem é quantitativa, utilizando a **Teoria do Enfoque Meta Analítico Consolidado (TEMAC)** (Mariano & Rocha, 2017). O TEMAC estabelece três etapas claramente definidas:

(1) preparação da pesquisa consiste na construção dos termos (*string*) da pesquisa de busca com palavras-chave que abordem o tema de forma mais apropriada. Também deve-se definir o campo espaço-tempo da pesquisa, as bases de dados e as áreas de conhecimento que serão utilizadas.

(2) apresentação e interrelação dos dados: nesta etapa, utiliza-se bibliometria para análise relacional entre os registros, com ênfase nas revistas mais relevantes, evolução temática e autores mais citados (Mariano & Rocha, 2017).

(3) detalhamento, modelo integrador e validação por evidências: na terceira etapa são necessárias análises mais profundas que permitam compreender melhor o tema, como a identificação de coautoria e cocitação, as principais abordagens, linhas de pesquisas e comparação dos resultados entre as fontes (Mariano & Rocha, 2017).

4. Resultado e discussões

Nos itens seguintes são apresentados e analisados os dados de acordo com cada etapa anteriormente descrita da TEMAC.

4.1. Etapa 1: Preparação da pesquisa

A busca bibliográfica foi conduzida entre os dias 10/07/2025 e 25/07/2025. As base de dados foram Web of Science – WoS - (webofscience.com), considerada como uma das melhores e mais completas bases de dados (Mariano & Rocha, 2017) e Scopus (https://www.scopus.com/), pela sua abrangência de dados e precisão no conteúdo (Adriaanse & Rensleigh, 2013) .

Como resultado, foram encontrados 32 resultados no Web of Science e 58 resultados na base do Scopus.

Tabela 1 - Termos pesquisados na pesquisa avançada
Fonte: elaborada pelos autores

Base de dados	Termos Pesquisados	Resultados
Web Of Science	TI=("public sector" OR "government agencies" OR "public administration" OR "government institutions" OR "public service" OR "civil service" OR "municipal government" OR "federal government" OR "Brazilian public sector") AND TS=("cybersecurity" OR "information security" OR "IT security" OR "data protection" OR "information systems security") AND TS=("top management" OR "senior management" OR executives OR "organizational leadership" OR board OR governance OR accountability OR responsibility OR "strategic oversight" OR "management support" OR "executive commitment")	32
Scopus	TITLE("public sector" OR "government agencies" OR "public administration" OR "government institutions" OR "public service" OR "civil service" OR "municipal government" OR "federal government" OR "Brazilian public sector") AND TITLE-ABS-KEY("cybersecurity" OR "information security" OR "IT security" OR "data protection" OR "information systems security") AND TITLE-ABS-KEY("top management" OR "senior management" OR executives OR "organizational leadership" OR board OR governance OR accountability	58

OR responsibility OR "strategic oversight" OR "management support" OR "executive commitment")

Foram definidos termos em português e inglês, priorizando a identificação de estudos que discutam a responsabilização da alta administração sobre a implementação da segurança da informação no setor público.

A pesquisa não impôs restrições de período ou área do conhecimento, visando maior abrangência diante da escassez de estudos específicos. Adicionalmente, não houve distinção entre os termos “segurança da informação”, “cibersegurança” e “privacidade”, dada a interdependência conceitual nos estudos sobre o tema.

4.2. Etapa 2: Apresentação e interrelação dos dados

Para (Mariano & Rocha, 2017), em revisões bibliométricas meta-analíticas, alguns resultados são tradicionalmente apresentados e seguem na sequência desta seção. Após a remoção dos resultados duplicados, foram encontrados 73 registros para compor a análise deste trabalho.

A Figura 1 mostra a evolução de publicações nas bases WoS e Scopus relacionadas ao tema. Observa-se um crescimento gradual das publicações a partir de 2016, sendo a base do Scopus em maior número. Quanto às citações, os picos ocorreram em 2015 e 2023, refletindo o interesse crescente pelo tema.

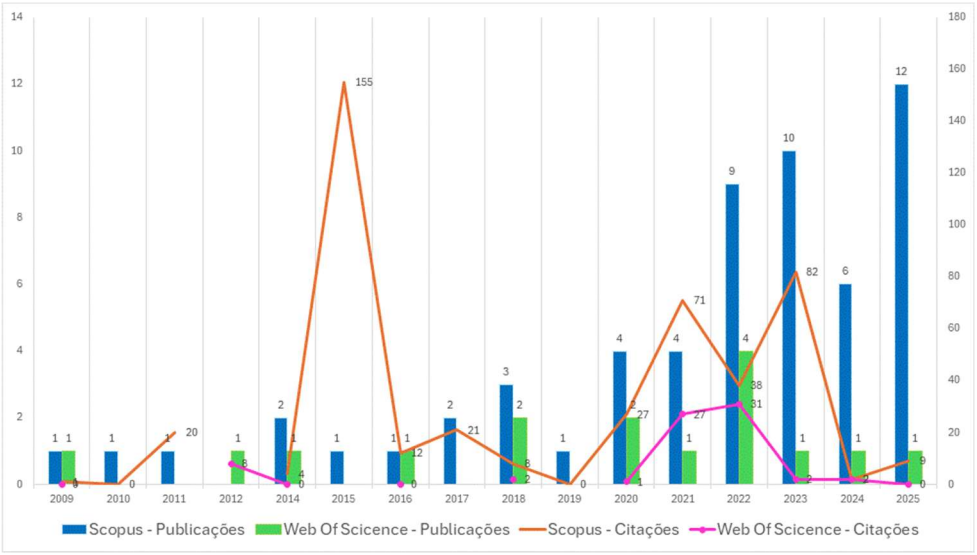

Figura 1 - Número de publicações e citações por ano
fonte: elaborada pelos autores

Ao concatenar as bases Scopus e WoS, foram identificados os trabalhos mais citados, Tabela 2. Os temas tratados por eles tiveram aspectos distintos, mas complementares quanto a governança digital e os desafios do serviço público: dificuldade de governança sobre grande volume de dados e falha de auditorias, especialmente quanto a responsabilidade pelos dados; desafio ao devido processo legal por decisões automatizadas na administração pública e a necessidade de responsabilização; governança cibernética como elemento central na transformação digital dos serviços públicos; interrelação entre governo eletrônico, cibersegurança e corrupção; decisões automatizadas poderiam ameaçar a legitimidade democrática, sugerindo mecanismos para mitigar riscos à confiança pública nas decisões automatizadas.

Tabela 2 - Autores mais citados
Fonte: elaborada pelos autores

No	Título	Autores	Ano	Citações
1	Government data does not mean data governance: Lessons learned from a public sector application audit	Thompson, N; Ravindran, R; Nicosia, S	2015	155
2	Administrative due process when using automated decision-making in public administration: some notes from a Finnish perspective	Suksi, M	2021	55
3	The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment	Mijwil M.M.; Filali Y.; Aljanabi M.; Bounabi M.; Al-Shahwani H.	2023	37
4	Nexus of E-government, cybersecurity and corruption on public service (PSS) sustainability in Asian economies using fixed-effect and random forest algorithm	Abbas, HSM; Qaisar, ZH; Xu, XD; Sun, CX	2022	31
5	The legitimacy gap of algorithmic decision-making in the public sector: Why it arises and how to address it	König, PD; Wenzelburger, G	2021	27

De acordo com as bases, 43 países realizaram trabalhos relacionados ao tema. Na Tabela 3 são apresentados os 10 países que mais publicaram. O Brasil divide a 7ª posição com outros 10 países por publicar 2 artigos.

No Brasil a pesquisa (Georg, Rodrigues, Alves, Silveira Júnior, & Nunes, 2022) investigou e mapeou os desafios enfrentados em segurança cibernética no setor público federal brasileiro, sob a perspectiva dos gestores de TI. Dentre vários achados importantes, estão a falta de governança efetiva e o distanciamento da alta administração dos temas de segurança cibernética.

A outra pesquisa brasileira, (Canedo, et al., 2022) aborda os desafios para evolução do grau de conformidade de um órgão federal em reação a aderência à LGPD. Identifica a necessidade de envolvimento interdepartamental para garantia da conformidade.

Tabela 3 - Número de Publicações por país

Fonte: elaborada pelos autores

Nº	Países	Publicações	%
1	Indonésia	6	8

2	EUA	4	5
3	Malásia	3	4
4	Espanha	3	4
5	Reino Unido	3	4
6	Albânia	2	3
7	Brasil	2	3
8	China	2	3
9	República Tcheca	2	3
10	Finlândia	2	3
11	Outros	45	3
	Total	**74**	**100**

Em relação as revistas que tiveram os trabalhos com maior número de citações (Tabela 4) *Government Information Quarterly* é a publicação de maior impacto no conjunto, com 155 citações. Em segundo lugar está *Artificial Intelligence and Law*, com 55 citações, seguida por *Mesopotamian Journal of CyberSecurity* com 37 citações. *Online Information Review* e *Technology in Society* apresentam números semelhantes, com 31 e 27 citações, respectivamente, ainda demonstrando relevância, mas em menor escala.

Tabela 4 - Revistas com maior número de citações
Fonte: elaborada pelos autores

Fonte da Publicação	Citações	IF	SCR	SJR	Quartil
GOVERNMENT INFORMATION QUARTERLY	155	10	11,1	2,861	Q1
ARTIFICIAL INTELLIGENCE AND LAW	55	3,1	-	0,815	Q1
Mesopotamian Journal of CyberSecurity	37	10,22	-	0,758	Q1
ONLINE INFORMATION REVIEW	31	3,5	3,7	1,025	Q1
TECHNOLOGY IN SOCIETY	27	12,5	11,5	2,559	Q1

A frequência de palavras-chave dos artigos selecionados é apresentada na Figura 2. Para obter a nuvem de palavras, foi utilizada a ferramenta TagCrowd (https://tagcrowd.com), que monta um diagrama com as palavras colocando em destaque as palavras mais observadas.

Figura 2 - Frequência de palavras-chave
Fonte: Elaborada pelos autores

Foram removidos da nuvem os termos utilizados na estratégia de busca (Tabela 1). As palavras com maior frequência aparecem em azul escuro e maior tamanho.

Os termos como "*data*", "*digital*", *"governance", "cl*oud" e *"technology"* destacam-se pela maior recorrência, sugerindo que esses conceitos representam eixos centrais das pesquisas no campo. A predominância de *"data"* e *"digital"* evidencia a ênfase das publicações em fenômenos associados à transformação digital e ao uso intensivo de dados. O termo *"governance"* complementa essa perspectiva, apontando o interesse das pesquisas em aspectos de governança de dados, políticas e estruturas organizacionais relacionadas à tecnologia da informação.

4.3. Etapa 3: Detalhamento, modelo integrador e validação por evidências

A apresentação e inter-relação dos dados, detalhamento, modelo integrador e validação por evidências, foram realizados por meio de mapeamento científico com o Software VosViewer (Centre for Science and Technology Studies, Leiden University, 2023 v.1.6.20).

Os dados extraídos das bases WoS e Scopus foram concatenados em uma terceira base única, permitindo a construção de mapas de densidade de calor para a análise das relações entre os itens.

Na Figura 3 é apresentada a análise de coautoria com o objetivo de mapear a rede de colaboração entre os autores. Aplicou-se um filtro mínimo de três citações aos 151 autores encontrados, evidenciando 59 com maior impacto na área, entre eles Afrune, Paolo e Angelleli, Mario (Catalano, et al., 2021), que se encontram em uma posição central com maior densidade de coautorias. Ambos estão vinculados ao *Department of Innovation Engineering, University of Salento*, ao *Cybersecurity Research Lab (CRlab), University of Salento*. Outro grupo relevante está associado *à Holistic AI e à University College London (UCL)*, incluindo os autores *Chaudhry A., Kazim E., Kingsman N., Hilliard A., Koshiyama A., Polle R*. e *Mohammed U* (Kingsman, et al., 2021)**.**

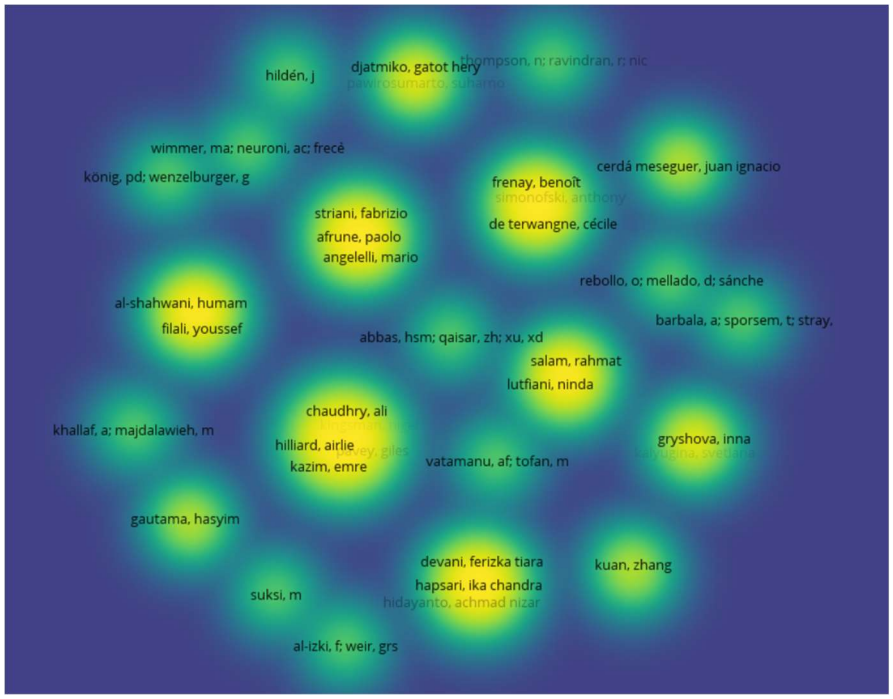

Figura 3 – Mapa de densidade de Coautoria
Fonte: Elaborada pelos autores

Na Figura 4 é apresentado o mapa de densidade de cocitação entre autores. Para esta visualização foi adotado um filtro mínimo de cinco citações. O mapa revela uma baixa densidade de interconexões entre os autores, com os nós distribuídos de forma dispersa. Destaca-se o autor Balaji, K., (Balaji, 2025) posicionado em uma área de maior intensidade, indicando maior frequência de citações. Também figuram no mapa, embora em regiões menos densas, os autores Mijwil, M. M., Kazim, E., Valero Torrijos, J., Bombardelli, M., Raharja, U. e Ponce, J., (Mijwil, Filali, Aljanabi, Bounabi, & Al-Shahwani, 2023) todos aparecendo em áreas isoladas. A ausência de agrupamentos indica baixa articulação entre os autores, sugerindo diversidade temática.

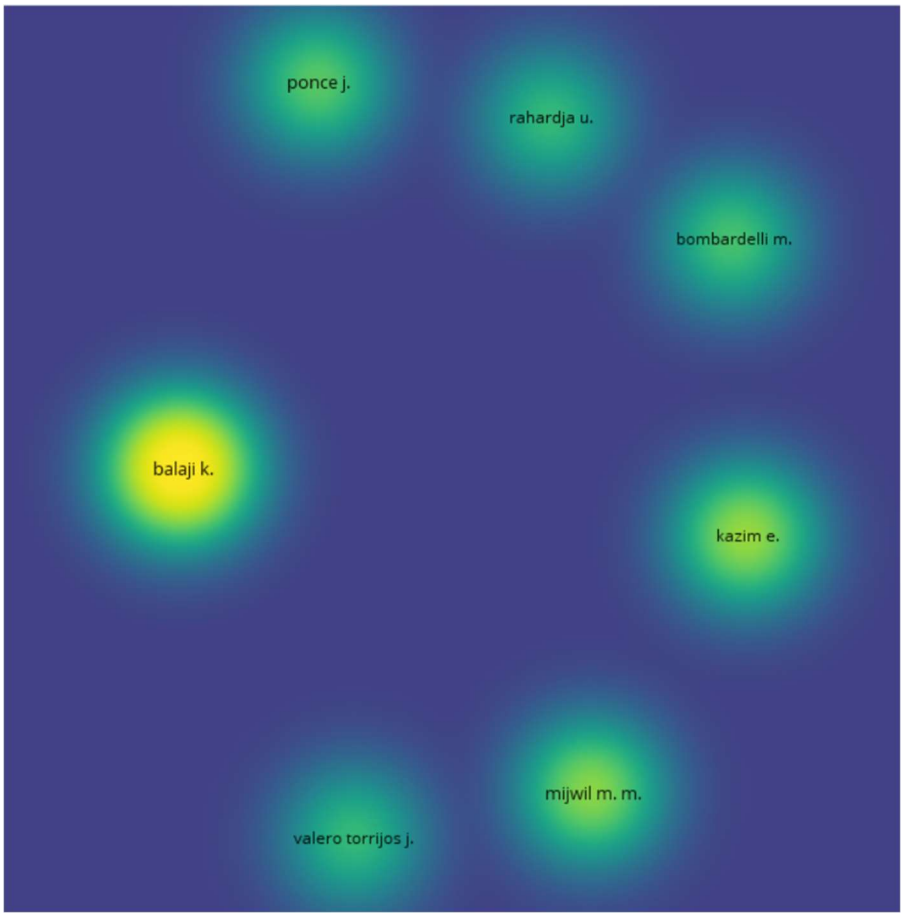

Figura 4 – Mapa de densidade de Cocitação
Fonte: Elaborado pela autora

No mapeamento de acoplamento bibliográfico por documento Figura 5, observa-se a formação de um cluster denso entre os trabalhos de (Mijwil, Filali, Aljanabi, Bounabi, & Al-Shahwani, 2023), (Pakhnenko & Kuan, 2023) e (Barbala, Sporsem, & Stray, 2023), sugerindo forte proximidade temática. Embora cada estudo aborde uma faceta distinta da transformação digital no setor público, todos compartilham

um eixo comum centrado em governança, ética e proteção de dados em contextos governamentais digitalizados.

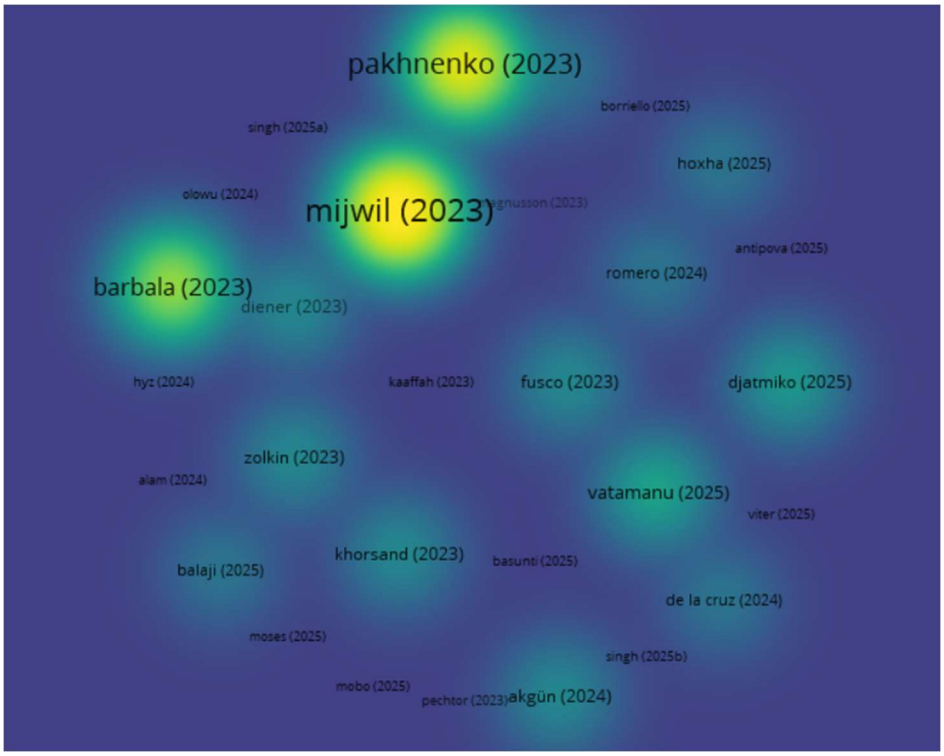

Figura 5 - Mapa de densidade de *bibliographic coupling*
Fonte: elaborada pelos autores

5. Discussão dos resultados

5.1. Governança e *accountability* em perspectivas internacionais

A análise internacional confirma a ausência de responsabilização clara da alta administração em segurança da informação, padrão igualmente observável no Brasil. Mesmo em países com elevado grau de maturidade em cibersegurança, os autores (Romanovská & Pitner, 2022) demonstram que prevalece uma abordagem

abstrata e pouco detalhada sobre os deveres de dirigentes e mecanismos de prestação de contas. Como explicitam os próprios autores:

> As estratégias são, em geral, muito abstratas, e a estratégia nacional australiana de cibersegurança não menciona as responsabilidades dos governos locais, como as cidades, enquanto os governos estaduais e territoriais são mencionados apenas de forma marginal. A estratégia belga de cibersegurança não menciona as regiões e suas responsabilidades, e a ilustração da governança belga em cibersegurança na estratégia não apresenta qualquer divisão vertical que inclua regiões e municípios (Romanovská & Pitner, 2022).

Para os autores, a adoção de um framework de governança multinível em cibersegurança, no qual a atribuição de responsabilidades é distribuída entre os diferentes níveis de governo, tem potencial para trazer efeitos positivos como o aumento da capacidade dos níveis superiores de governo para resolver problemas complexos, monitorar e adaptar serviços aos níveis inferiores e, indiretamente, elevar a conscientização pública sobre segurança digital.

Em outro estudo sobre o cumprimento das práticas de segurança em municípios e regiões suecas, evidenciou-se que a ausência de governança e gestão compromete a resiliência organizacional frente a incidentes. Os autores observam que "Análises de segurança pós-incidente após eventos como os ataques à Equifax, Capital One e SolarWinds apontaram claramente que falhas de governança foram a principal causa dos roubos de dados ocorridos" (Magnusson, Dalipi, & Elm, 2023). O estudo destaca, de forma positiva, que a busca pelas melhores práticas, padrões internacionais e requisitos regulatórios vem promovendo avanços importantes na redução de riscos cibernéticos no setor público.

No mesmo sentido, conforme ressaltado por (Suksi, 2021), é fundamental que sempre seja possível definir, de forma inequívoca, o status legal daqueles que estão no comando e são responsáveis pelas decisões tomadas, inclusive quando se utilizam sistemas automatizados. A ausência dessa definição mina a *accountability* e dificulta

a responsabilização da alta administração, vulnerabilizando os processos de adoção e fiscalização das políticas de segurança da informação.

Nesse contexto, o artigo de (Vatamanu & Tofan, 2025) contribui para a discussão e coloca o *accontability* como forma de garantir a transparência e ética do serviço público. Os autores afirmam que "Estruturas de compliance e accountability são essenciais para garantir que as tecnologias de inteligência artificial sejam utilizadas de forma responsável e que a administração pública permaneça transparente e ética" (Vatamanu & Tofan, 2025). Embora o texto não direcione essa exigência especificamente à alta administração, tampouco a exclui de forma implícita. O artigo reforça a premissa de que a responsabilização deve estar presente em todos os níveis hierárquicos — inclusive nos cargos de direção superior — como condição para a eficácia das políticas públicas. Dessa forma, mesmo sem nominar diretamente os gestores de topo, o estudo corrobora a importância de mecanismos formais que alcancem também os dirigentes, alinhando-se, ainda que de modo indireto, à crítica sobre a omissão normativa que dificulta a responsabilização da alta cúpula nos projetos de segurança da informação no setor público.

5.2. Desafios de implementação: auditorias, maturidade e diagnóstico brasileiro

Outro ponto que merece destaque é que, apesar da existência de normas e políticas de segurança da informação baseadas em padrões internacionalmente reconhecidos, falhas na implementação acabam comprometendo a responsabilização e o controle sobre os ativos de informação. Auditorias recentes em órgãos australianos evidenciaram que problemas recorrentes, como a impossibilidade de rastrear responsáveis por inserções e alterações de dados sensíveis, não decorrem apenas de limitações técnicas ou legislativas, mas fundamentalmente da falta de uma estrutura robusta de governança e *accountability*, dificultando inclusive a atribuição de responsabilidades à alta administração (Thompson, Ravindran, & Nicosia, 2015).

No contexto da segurança cibernética no setor público federal brasileiro, estudos nacionais revelam que, em muitos órgãos públicos, a governança de segurança cibernética é incipiente ou inexistente, marcada pelo distanciamento dos dirigentes máximos em relação aos processos de TI e pela ausência de políticas específicas ou modelos definidos de governança de segurança (Georg, Rodrigues, Alves, Silveira Júnior, & Nunes, 2022). Essa pesquisa realizada no setor público federal, abrangendo as três esferas de poder, entrevistou gestores de TI ou de segurança da informação que relataram a falta de estruturas formais de governança de segurança cibernética nos órgãos e que os executivos de topo raramente se envolvem ativamente nessas questões, resultando em baixo alinhamento estratégico entre as iniciativas de segurança e os objetivos organizacionais (Georg, Rodrigues, Alves, Silveira Júnior, & Nunes, 2022).

Essa percepção é corroborada por um diagnóstico recente nos âmbitos estadual e federal: benchmarkings conduzidos pelo Banco Interamericano de Desenvolvimento apontam que 30% dos governos estaduais brasileiros não possuem sequer um analista de cibersegurança, e apenas 22% contam com a figura de um *Chief Information Security Officer* (CISO) em sua estrutura (Santiago Paz, 2025). Esses números indicam uma carência significativa de liderança institucional dedicada à segurança da informação. Mesmo onde há alguma estrutura estabelecida, o alinhamento estratégico permanece deficiente, em parte pela baixa percepção, por parte da alta administração (CISO), da relevância da segurança cibernética para o alcance das metas organizacionais.

Recentemente o TCU apresentou, no Acórdão 2.387/2024 (Tribunal de Contas da União, 2024), dados sobre governança incipiente, que podem ser resultado direto da falta de envolvimento da alta administração na condução do tema segurança da informação nos órgãos do SISP. Das 229 organizações que responderam ao ciclo 1 ou 2, do PPSI, nenhuma delas implementa as 56 medidas de segurança do IG1, somente 14 implementam mais de 70% e apenas duas organizações implementam

mais de 90%. Como consequência desse cenário, tem-se que as organizações do SISP não estão protegidas contra os ataques cibernéticos mais comuns, uma vez que o IG1 é definido como o conjunto básico de medidas de segurança de defesa cibernética que todas as organizações deveriam aplicar para se proteger contra esses ataques.

5.3. Intervenções regulatórias e recomendações estratégicas

No cenário internacional, um estudo do leste europeu defende a implementação de um sistema abrangente de proteção cibernética no setor público (Viter, Guzonova, Shevchuk, Molochko, & Kutova). Tal sistema deve estar alinhado aos padrões internacionais da OTAN e da União Europeia e deve abranger todos os níveis da administração pública, exigindo reformas tanto no arcabouço normativo quanto na cultura gerencial de maneira a funcionar adequadamente. Um dos principais pontos do trabalho é a ênfase na criação de mecanismos de responsabilização, evidenciada pela afirmação de que é necessário "implementar controle e responsabilização por violações à segurança da informação em todos os níveis da administração pública" (Viter, Guzonova, Shevchuk, Molochko, & Kutova). Essa ausência de responsabilização clara reforça a crítica de que a omissão normativa e prática por parte dos dirigentes públicos constitui um entrave significativo à efetiva implementação das políticas de segurança da informação. A obra também ressalta que, sem mudanças estruturais na gestão e na transparência dos processos, os riscos institucionais como corrupção, mau uso de recursos e perda de confiança pública tendem a se perpetuar, comprometendo os objetivos estratégicos da cibersegurança governamental.

No Brasil, a fragilidade na responsabilização da alta administração é evidenciada em diferentes auditorias do TCU. Embora tratem de temas distintos, os acórdãos 2.387/2024 (Tribunal de Contas da União, 2024) e 2.430/2024, (Tribunal de Contas da União, 2024) revelam um padrão de insuficiência normativa que dificulta a responsabilização direta dos gestores de alto escalão. No primeiro, o TCU apontou a ausência de previsão normativa clara que atribua responsabilidade à alta

administração pela gestão dos riscos cibernéticos (Tribunal de Contas da União, 2024). No segundo, evidenciou que a Política Nacional de Cibersegurança (PNCiber), apesar de instituída por decreto, não dispõe de uma estrutura de coordenação com autoridade e prerrogativas suficientes para sua execução em âmbito nacional (Tribunal de Contas da União, 2024), o que fragiliza a governança cibernética. O próprio TCU esclarece, em resposta à Consulta nº 382507/2025, que a responsabilização de gestores depende da existência de pressupostos legais definidos na Lei nº 8.443/1992 (Presidência da República, 1992), entre eles: a comprovação de nexo causal entre conduta e ao dano ao erário, a ocorrência de dolo ou culpa, e a violação de norma legal por **ação** ou **omissão** (grifos nossos).

Para contribuir na definição da "**ação** ou **omissão**" passível de punição, no Acórdão 2.387/2024 o TCU recomendou à SGD que aperfeiçoe o instrumento do PPSI - (Brasil. Ministério da Gestão e da Inovação em Serviços Públicos, 2023) explicitando a responsabilidade da alta administração (Tribunal de Contas da União, 2025). Também recomendou a cada uma das organizações do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP - (Brasil, 2011) que o processo de gestão de riscos decorrentes de ataques cibernéticos seja liderado explicitamente pela sua alta administração (Tribunal de Contas da União, 2024).

5.4. Engajamento da alta administração e cultura organizacional

O estudo de (De La Cruz, et al., 2024) amplia o debate ao abordar a importância do engajamento efetivo da alta administração. A pesquisa, conduzida no contexto do setor público norte-americano, analisou os fatores críticos para o sucesso de sistemas de análise de dados em cibersegurança e concluiu que o apoio da alta gestão (*Top Management Support – TMS*) é determinante para a implementação e uso eficaz dessas tecnologias. Segundo os autores:

> O apoio da alta administração (Top Management Support – TMS) é fundamental para a implementação e utilização bem-sucedidas de sistemas de análise de dados em cibersegurança nas organizações governamentais dos Estados Unidos. O TMS

> envolve a priorização, o endosso e a alocação de recursos pelas lideranças seniores às iniciativas de cibersegurança, o que integra a segurança digital à estratégia e à cultura organizacional, aumentando a eficácia das medidas de proteção. [...] Apesar de desafios como restrições orçamentárias e exigências regulatórias, o TMS desempenha um papel essencial na superação desses obstáculos, na defesa das prioridades em cibersegurança e na garantia do alinhamento estratégico" (De La Cruz, et al., 2024).

Como efeito positivo, o estudo demonstra que o apoio da alta administração contribui significativamente para a implementação e eficácia das tecnologias *(Cybersecurity Data Analytics Systems – CDAS)*, criando um ambiente favorável a resiliência institucional diante das ameaças digitais.

Os achados de (De La Cruz, et al., 2024) reforçam que, embora o papel da alta administração seja comumente reconhecido por sua atuação no alinhamento estratégico e na alocação de recursos, é o envolvimento efetivo e contínuo da liderança que se mostra determinante para consolidar a segurança da informação como um elemento estruturante da cultura organizacional. Nesse sentido, a literatura respalda a necessidade de protagonismo da alta gestão não apenas na formulação inicial das políticas de segurança, mas também na sua sustentação, monitoramento e aprimoramento. A governança em cibersegurança deve ser entendida como um processo contínuo, fundamental para a consolidação de práticas seguras, alinhada à seleção de gestores confiáveis e experientes para conduzir a gestão do ambiente digital (Mijwil, Filali, Aljanabi, Bounabi, & Al-Shahwani, 2023). Fragilidades estruturais nesse aspecto comprometem a efetividade das políticas de segurança, dificultando a resposta coordenada a ameaças.

6. Conclusão

Este artigo analisou os desafios para a implementação da segurança da informação no serviço público brasileiro, com ênfase na responsabilização da alta administração. Para isso, a pesquisa utilizou a Teoria do Enfoque Meta-analítico Consolidado

(TEMAC) como método de revisão sistemática da literatura. A abordagem permitiu identificar padrões recorrentes na literatura sobre responsabilização e seus impactos.

A análise permitiu identificar que, no contexto internacional, a responsabilização da alta gestão ainda é tratada de forma abstrata e pouco vinculada a mecanismos legais de prestação de contas. Neste cenário, *accountability* é reconhecido como componente estruturante da ética e transparência pública, devendo atingir todos os níveis hierárquicos, inclusive a alta administração. A ausência de mecanismos formais que assegurem essa responsabilização está associada a riscos institucionais como corrupção, mau uso de recursos e à fragilização das estruturas de controle.

No cenário brasileiro, constatou-se a baixa participação da alta administração nas decisões relacionadas à segurança da informação, bem como carência de liderança institucional dedicada ao tema e baixa percepção, por parte da alta administração, quanto a sua relevância estratégica. Adicionalmente, o exame dos acórdãos recentes do TCU constatou fragilidades normativas que dificultam a responsabilização direta da alta administração pela gestão dos riscos cibernéticos. A explicitação dessas responsabilidades e a exigência de liderança ativa da alta gestão no processo de gestão de riscos decorrentes de ataques cibernéticos, são medidas que possibilitam a superação das atuais limitações normativas, contribuindo para o fortalecimento da governança cibernética dos órgãos públicos brasileiros.

Diante das evidências reunidas, o estudo contribui para o mapeamento de entraves normativos e institucionais relacionados à responsabilização da alta administração em segurança da informação. Tais achados podem subsidiar pesquisas sobre modelos regulatórios e mecanismos de conformidade aplicáveis à administração pública.

Reconhece-se que essa pesquisa apresenta limitações: a base bibliométrica concentrou-se em periódicos indexados nas bases Scopus e WoS, o que pode limitar a amostra, mesmo sem delimitarmos o escopo temporal e área de conhecimento.

Como trabalhos futuros, sugere-se estudos de caso longitudinais que avaliem a evolução de indicadores antes e depois da introdução de métricas de responsabilização executiva em diferentes contextos institucionais, permitindo avaliar seus impactos sobre os níveis de maturidade em segurança da informação.

Referências

ABNT. (2023). ABNT NBR ISO/IEC 27032:2023 — Segurança cibernética – Diretrizes para segurança na Internet. Rio de Janeiro: ABNT.

ABNT. (2023). ISO/IEC 27000:2023 – Information technology – Security techniques – Information security management systems – Overview and vocabulary. Geneva: ISO.

Adriaanse, L., & Rensleigh, C. (2013). Web of Science, Scopus and Google Scholar: A content comprehensiveness comparison. doi:10.1108/EL-12-2011-0174

Alves, R. S., Georg, M. A., & Nunes, R. R. (s.d.). Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros. doi:10.5281/zenodo.8032915

Balaji, K. (2025). E-Government and e-governance: Driving digital transformation in public administration. Em I. Global (Ed.), *Public Governance Practices in the Age of AI* (pp. 23-44). doi:10.4018/979-8-3693-9286-7.ch002

Barbala, A., Sporsem, T., & Stray, V. (2023). Data-Driven Development in Public Sector: How Agile Product Teams Maneuver Data Privacy Regulations. *24th International Conference on Agile Software Development (XP 2023). 475*, pp. 165-180. Amsterdam, Netherlands: Springer International Publishing AG. doi:10.1007/978-3-031-33976-9_11

Brasil - Presidência da República. (2018). *Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)*. Fonte: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Brasil - Secretaria de Governo Digital. (2023). *Guia de Referência para Elaboração do Plano de Proteção de Segurança da Informação – PPSI*. Brasilia.

doi:https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf

Brasil. (2011). *Decreto nº 7.579, de 11 de outubro de 2011*. Fonte: Planalto: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/decreto/d7579.htm

Brasil. (2017). *Decreto nº 9.203, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional*. Fonte: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9203.htm

Brasil. Ministério da Gestão e da Inovação em Serviços Públicos. (2023). *SGD/MGI nº 852, de 28 de março de 2023*. Fonte: Governo Federal: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-474164307

Canedo, E. D., Ribeiro, V. C., Cerqueira, A. J., Gravina, R. M., Camões, R., Dos Reis, V. E., . . . De Sousa, R. T. (2022). Evaluating and Evolving the Compliance to the Brazilian General Data Protection Law in a Federal Government Agency. *Lecture Notes in Business Information Processing, 455*. doi:10.1007/978-3-031-08965-7_1

Catalano, C., Afrune, P., Angelelli, M., Maglio, G., Striani, F., & Tommasi, F. (2021). Security testing reuse enhancing active cyber defence in public administration., (pp. 120-132). Virtual, Online.

Center for Internet Security. (s.d.). *CIS Critical Security Controls*. Fonte: Center for Internet Security: https://www.cisecurity.org/controls

Centre for Science and Technology Studies, Leiden University. (2023 v.1.6.20). *VOSviewer: Visualizing Scientific Landscapes*. Fonte: https://www.vosviewer.com/

De La Cruz, E., Gonaygunta, H., Oni, O., Meduri, S. S., Nadella, G. S., & De La Cruz, A. M. (2024). Cybersecurity Data Analytics System Success: An Exploratory Study on U.S. Government Agencies. *Preprint – ResearchGate*. doi:10.1109/iSemantic63362.2024.10762173

Ferreira, L. V. (2022). Cybersecurity and Ransomware in the Brazilian Government. *InterAção, v. 15*, pp. 107–123.

Georg, M. A., Rodrigues, W. M., Alves, C. A., Silveira Júnior, A., & Nunes, R. R. (nov de 2022). Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. *Revista Ibérica de Sistemas e Tecnologias de Informação*, pp. 602-616. doi:10.5281/zenodo.7855320

Gil, A. C. (2017). *Métodos e técnicas de pesquisa social* (6 ed.). São Paulo: Atlas.

Goldoni, L. R., Rodrigues, K. F., & Medeiros, B. P. (2023). Qual é o futuro da governança de cibersegurança no Brasil? *SciELO*. doi:10.12660/cgpc.v29.90972

Kingsman, N., Kazim, E., Chaudhry, A., Hilliard, A., Koshiyama, A., Polle, R., . . . Mohammed, H. U. (2021). Exploring the Governance of Algorithmic Decision-Making: A Multi-Stakeholder Perspective on Auditability. *2021 AAAI/ACM Conference on AI, Ethics, and Society (AIES 2021)*, (pp. 162-172). Virtual, online.

Laginestra, A. (2021). *Cibersegurança no Território Brasileiro: Impacto da LGPD e normas de Segurança da Informação na Defesa Nacional* (1 ed.). Rio de Janeiro: Biblioteca de Segurança.

Magnusson, L., Dalipi, F., & Elm, P. (2023). Cybersecurity compliance in the public sector: are the best security practices properly addressed? Em *Communications in Computer and Information Science* (pp. 370–384). doi: https://doi.org/10.1007/978-3-031-36001-5_28

Mariano, A. M., & Rocha, M. S. (2017). Revisão da Literatura: Apresentação de uma Abordagem Integradora. *XXVI Congreso Internacional AEDEM | 2017 AEDEM International Conference - Economy, Business and Uncertainty: ideas for a European and Mediterranean industrial policy?* (pp. 427-443). Reggio Calabria: AEDEM.

Mijwil, M. M., Filali, Y., Aljanabi, M., Bounabi, M., & Al-Shahwani, H. (2023). The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. (M. A. Press, Ed.) *Mesopotamian Journal of CyberSecurity*, pp. 1-6. doi:10.58496/MJCS/2023/001

Nakamura, E. T. (2024). O papel da segurança cibernética no universo digital: a importância do fator humano. Rio de Janeiro: Instituto de Pesquisa Econômica Aplicada (Ipea). doi:http://dx.doi.org/10.38116/9786556350660cap9

OECD – Organisation for Economic Co-operation and Development. (2020). *OECD Public Integrity Handbook*. Paris: OECD Publishing.

Pakhnenko, O., & Kuan, Z. (2023). Ethics of Digital Innovation in Public Administration. *Business Ethics and Leadership*, pp. 113-121. doi: 10.21272/bel.7(1).113-121.2023

Presidência da República. (1992). *Lei nº 8.443, de 16 de julho de 1992*. Fonte: Lei Orgânica do Tribunal de Contas da União: https://www.planalto.gov.br/ccivil_03/leis/l8443.htm

Ribeiro, M. M., & Segatto, C. I. (2025). Inteligência artificial nas organizações públicas brasileiras: heterogeneidades e capacidades em tecnologia da informação. *Revista de Administração Pública (RAP),* doi:10.1590/0034-761220240066x

Romanovská, F., & Pitner, T. (2022). Multi-Level Cybersecurity Governance Frameworks for Public Administration. *roceedings of IDIMT-2022*, pp. 277-284. doi:DOI: 10.35011/IDIMT-2022-277

Santiago Paz, M. L. (2025). Cibersegurança nos estados brasileiros: diagnóstico e recomendações. *Banco Interamericano de Desenvolvimento*.

Santos, R. B., & Silva, T. B. (2021). Gestão da segurança da informação e comunicações: análise ergonômica para avaliação de comportamentos inseguros. *Revista Brasileira de Segurança da Informação*. doi:10.20396/rdbci.v19i00.8665529

Serpa, D. (2024). Transformação digital da inteligência nacional brasileira. *Revista Brasileira de Inteligência (ABIN)*.

Silva, M. A., & Santos, F. R. (2020). *Fundamentos da Governança, Riscos e Compliance*. São Paulo: Atlas.

Suksi, M. (2021). Administrative due process when using automated decision-making in public administration: some notes from a Finnish perspective. *Artificial Intelligence and Law, 29*, pp. 87-110. doi:10.1007/s10506-020-09269-x

Thompson, N., Ravindran, R., & Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. *Government Information Quarterly, 32*, pp. 316-322. doi:10.1016/j.giq.2015.05.001

Tribunal de Contas da União. (2020). *Referencial Básico de Governança Organizacional: aplicações ao setor público*. TCU, Brasília. Fonte: https://portal.tcu.gov.br/data/files/FB/B6/FB/85/1CD4671023455957E18818A8/Referencial_basico_governanca_organizacional_3_edicao.pdf

Tribunal de Contas da União. (2024). *Acórdão nº 2387/2024 – Plenário*. Brasília: Tribunal de Contas da União. Fonte: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/NUMACORDAO%253A2387%2520ANOACORDAO%253A20

24%2520COLEGIADO%253A%2522Plen%25C3%25A1rio%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0

Tribunal de Contas da União. (2024). *Acórdão nº 2430/2024 – Plenário*. Brasília: Tribunal de Contas da União.

Tribunal de Contas da União. (2025). *Resposta à manifestação nº 382507 enviada à Ouvidoria do TCU*. Brasília: TCU. Fonte: https://pesquisa.apps.tcu.gov.br/pesquisa/acordao-completo

Vatamanu, A. F., & Tofan, M. (2025). Integrating Artificial Intelligence into Public Administration: Challenges and Vulnerabilities. *Administrative Sciences, 15*. doi:10.3390/admsci15040149

Viter, D., Guzonova, V., Shevchuk, V., Molochko, T., & Kutova, M. (s.d.). Mechanisms of public administration to ensure national and information security. *Management Theory and Studies for Rural Business and Infrastructure Development, 47*. doi:10.15544/mts.2025.20